Please enter amendment /A.S./ 09/30/10

AMENDMENTS TO THE SPECIFICATION

Please amend the title as follows:

Reconstruction of Program Streams Split Across Multiple Packet ~~Program~~ Identifiers

Please amend the paragraph starting at page 2, line 17 as follows:

This invention relates generally to the field of multiply encoded program data streams identified by multiple packet ~~program~~ identifiers (PIDs). More particularly, in certain embodiments, this invention relates to reconstitution of multiple encrypted multiple carriage program data streams.

Please amend the paragraph starting at page 3, line 23 as follows:

In a conventional cable system, system information (SI) is provided in the form illustrated in **FIGURE 1** of a Program Association Table (PAT) which contains an entry for each program. Each program in the PAT has a pointer to a particular Program Map Table (PMT) such as 12, 14, ... 18 and 20 associated with the particular program. The PMT table contains packet ~~Program~~ Identifiers (PIDs) that are associated with the elementary streams for each program.

Please amend the paragraph spanning pages 3 and 4 as follows:

In the above-referenced patent applications, the multiple sets of encrypted packets representing the encrypted portions of the partially encrypted programs are distinguished from one another by use of distinctive packet ~~program~~ identifiers (PIDs). Thus, for example, two encrypted portions of a program have two unique PIDs - a primary PID and a shadow (or secondary) PID. In order for the receiving equipment to determine which PIDs are associated with a particular encryption scheme, the PID information is transmitted from the cable system (or other distributor) headend. In one embodiment, illustrated in **FIGURE 2**, this can be done using a duplicate set of system information (SI) to identify the various PIDs. In this example, two separate PATs 30a and 30b are used to associate programs with PMTs ~~with PATs~~ 32a, 34a, ...38a and 40a in the case of PAT 30a, and with 32b, 34b,...38b and 40b in the case of PAT 30b. Each receiving system is able to detect and process whichever SI is appropriate. The system Application No.: 10/084,106

(e.g., the cable system headend) generating the SI creates duplicate SI for each encryption scheme used. When bandwidth is critical, the extra packets used to transmit the duplicate SI may be difficult to accommodate.

Please amend the paragraph starting at page 8, line 17 as follows:

Whenever a shadow packet is received and sent to buffer 116, the interrupt service routine toggles switch 128 to effectively change primary packet buffers at the shadow PID boundary. This limits the range of primary packets that the software must search in order to find the packet to be replaced by the shadow packet. Depending upon whether the headend places the shadow packet in the data stream just prior to or just after the corresponding encrypted packet having the primary PID, the corresponding packet can be found either at the end of one ~~end one~~ primary packet buffer or the beginning of the other. Latency impacts are minimized since processing occurs within very few packet times and processing bandwidth is minimized since only one or two packets must be scanned by software to identify the correct packet.

Please amend the paragraph starting at page 10, line 10 as follows:

Thus, a method of constructing a stream of data packets having primary and shadow packet identifiers (PIDs), the packets having headers and payloads consistent with certain embodiments of this invention includes ~~include~~ receiving an incoming data stream having packets with the primary and shadow PIDs; providing a stream of packets having the primary PID to a first buffer; detecting a packet having the shadow PID and a shadow payload in the incoming data stream; switching the stream of packets having the primary PID to a second buffer in response to the detecting; and searching a first packet stored in the second buffer and a last packet stored in the first buffer for a packet corresponding to the packet having the shadow PID.